Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 9 pp. 4214-4223, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.9.4214

익명 게시판 환경에서 가상 아이디를 이용한 개인정보보호에 관한 연구

민소연[1*], 장승재[2]
[1]서일대학교 정보통신과, [2]숭실대학교 컴퓨터학과

A Study on the protection of personal information using a Virtual IDs in an anonymous bulletin board

So-Yeon Min[1*] and Seung-Jae Jang[2]
[1]Dept. of Information and Communication, Seoil College
[2]Dept. of Computer Science, Soongsil University

요 약 최근 인터넷 게시판의 실명 및 익명 사용에 대한 논쟁은 주요 이슈가 되고 있다. 실명을 사용할 경우 자유로운 토론 및 프라이버시 침해할 우려가 있는 반면에, 익명을 사용하는 경우에 있어서는 악성 댓글 폭력이라든지, 존재하지 않는 허위 사실 유포 등의 인터넷의 역기능이 나타날 수 있다. 따라서 본 논문에서는 SSO의 기술 중 하나인 XML 토큰 방식을 사용하여 개인정보의 분산을 막고 단일 로그인이 가능하게 하였고 토큰 발급 시 가상 아이디와 경로구성을 통해 익명성 및 조건부 추적이 가능한 익명 게시판을 제안 하였다. 성능분석 결과 접속자 수에 따른 인증시간에서 그룹 서명 방식을 사용한 익명 게시판은 평균 응답 속도가 0.72초, 제안하는 방식은 0.18초를 나타내었다. 즉 인증시간에서 4～5배 정도 빠른 응답 속도를 보였다. 또한 제안하는 시스템은 단일 인증을 제공하고 사용자가 서명을 하지 않아도 되기 때문에 사용자 편의성에서 월등히 뛰어나며, 익명 게시판 환경에서의 사용자 편의성은 제안하는 시스템이 더 적합함을 알 수가 있었다.

Abstract The argument related to the use of real and anonymous names on the Internet bulletin board has recently become a main issue. When using real names, it is possible to violate free discussion and privacy. Also, when using anonymous names, it is possible to have the reverse function of the Internet in regard to the use of malicious replies or the distribution of false ideas. Therefore, this paper has made it possible to prevent the spread of the user's personal information and execute the single log-in process by using the XML-token method which is one of the SSO technologies. Also, by issuing virtual IDs and forming the path when establishing tokens, the anonymous bulletin board which provides anonymity with a conditional tracing process has been suggested. After analyzing the performance of visitor numbers at authentication time, the anonymous bulletin board based on the group signature method showed the average response rate of 0.72 seconds, 0.18 seconds, which was suggested scheme. In the authentication time 4-5 times faster response speed, respectively. Also, since the suggested system does not have to provide a single authentication process or make the user provide his or her signature, the level of user's convenience seems to be much higher. Such a result shows that the system suggested on the anonymous bulletin board has a more appropriate level of user's convenience.

Key Words : Anonymous Authentication, SSO(Single Sign On), Virtual ID

본 논문은 2011년도 서일대학 학술연구비에 의해 연구되었습니다.
*Corresponding Author : So-Yeon Min
Tel: +82-10-6576-0726 email: symin@seoil.ac.kr
접수일 12년 07월 11일 수정일 12년 08월 14일 게재확정일 12년 09월 06일

1. 서론

현재 인터넷 게시판에서는 기본적으로 주민등록번호를 포함한 개인정보를 통해서 실명 등록을 한 후, 해당 계정으로 로그인 후 게시판을 사용하도록 하는 제한적 본인 확인제(이하 '인터넷 실명제')가 실행되고 있다. 이것은 인터넷 게시판에서 실명을 사용할 경우 자유로운 토론이 어려우며 결과적으로 사용자 프라이버시를 침해할 우려가 있는 반면, 익명을 사용할 경우 자유로운 토론은 가능하지만 악성 댓글 폭력이라든지, 존재하지 않는 허위 사실 유포 등의 인터넷의 역기능이 있을 수 있기 때문이다[1]. 2007년 방송통신위원회에서는 후자를 더 큰 위험으로 판단하고 이를 막기 위해 인터넷 실명제를 내놓았다. 하지만 사이버 범죄를 방지하기 위한 목적으로 만들어진 인터넷 실명제는 불필요하게 과도한 사용자의 개인정보를 요구하여 개인의 사생활을 침해하고, 부주의한 정보관리로 인해 대량의 개인정보 유출의 근원이 되었다. 또한 게시판 서비스를 이용하기 위해서는 사용자 개인 정보 등록을 포함하는 가입 절차가 요구되기 때문에 웹 사이트마다 개인 정보가 중복적으로 존재하여 개인 정보 유출에 대한 우려가 증폭되고 있는 상황이다[3]. 이 때문에 사용자들은 틀린 정보를 입력하는 경우가 많다. 이러한 상황은 단순한 사용자의 불편을 넘어서 서비스 이용의 확산을 가로막고 개인정보의 도용이나 프라이버시 침해 같은 심각한 문제를 야기할 수 있다.

최근에는 개인정보보호의 방법으로 익명인증(anonymous authentication)과 인터넷에 산재한 아이디와 개인정보들을 적절히 관리해줄 인터넷 ID관리 서비스에 대한 연구가 활발하게 진행되고 있다[6]. 익명인증은 불필요한 개인의 신분노출을 피하면서 사용자의 정당성을 인증한다. 그러나 Blind Signature, Group Signature 등 기존의 익명인증 방법들을 공개키 기반 구조를 가지고 있기 때문에 전자투표, 전자입찰 등 프라이버시에 민감한 응용에는 적합하지만 익명 게시판에 사용하기는 부담스럽다. 때문에 사용자의 ID 정보를 저장, 관리하며 이를 통해 단일 인증, 개인정보 보호를 제공하는 인터넷 ID 관리 서비스를 적절히 이용하여 익명 게시판에 사용할 수 있는 보다 효과적인 보안 인증 체제를 찾아야 할 것이다.

본 연구에서는 개인 정보를 서로 공유하고 관리하는 SSO(Single Sign On)의 기술 중 하나인 토큰방식을 사용하여 개인정보의 분산을 막고 단일 로그인이 가능하게 하는 방법을 제안한다. 또한 토큰 발급 시 가상 아이디와 경로 구성을 통해 조건부 추적이 가능한 익명 게시판을 제안한다. 또한 토큰을 사용한 단일인증 기법을 사용함으로써 무분별한 회원가입을 통한 개인정보 누출을 막도록 설계한다. 또한 토큰을 사용한 단일인증 기법을 사용함으로써 무분별한 회원가입을 통한 개인정보 누출을 막도록 설계한다. 암호화 기법은 토큰의 무결성을 보장하기 위해 XML 전자서명을 하고 경로의 기밀성을 보장하기 위해 인증기관의 비밀키로 암호화 한다. XML 전자서명은 RSA 1024bit 공개키 알고리즘을 사용하였고 경로 암·복호화로는 AES 256bit 대칭키 알고리즘을 사용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 익명인증 기술들과 SSO(Single Sign-On)와 같은 기존의 기법에 대해 분석하였다. 3장에서는 익명 게시판을 위한 가상 아이디 발급과 경로 구성 방법을 제안하였고, 4장에서는 구현 결과와 기존 시스템과 비교 분석한 결과를 기술 하였다. 마지막으로 5장에서는 본 논문에 시스템 결과 평가를 바탕으로 한 결론과 향후 연구 방향에 대해 기술하였다.

2. 관련연구

2.1 익명인증의 정의

익명 인증은 1985년 David Chaum이 제안한 익명 신용장(Anonymous Credential) 시스템에서 기인한 전자서명을 이용한 인증 방법이다. 익명인증은 초기 전자화폐, 전자투표 등과 같은 분야의 응용을 위해 연구되었고, 대부분이 이론적인 연구에 그쳤으나, 최근에는 개인정보의 보호방법으로 익명인증에 대한 연구가 활발히 진행되고 있다[11-18]. 익명인증의 전자서명 방식으로 은닉 서명(Blind Signature), 그룹 서명(Group Signature), 링 서명(Ring Signature), 추적가능 서명(Traceable Signature)등의 방법들이 제안되어 연구되고 있다.

2.2 익명인증 기술

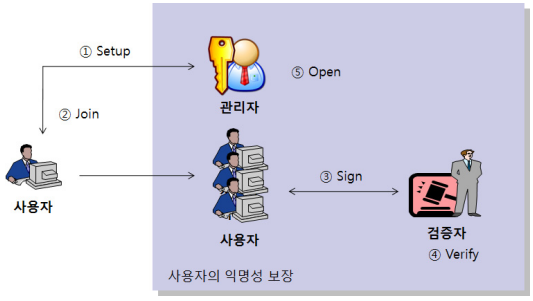
2.2.1 은닉 서명

1982년에 David Chaum이 제안한 전자 서명의 한 형태로써 서명자가 메시지 내용을 모르고 서명을 하도록 한다. 기본적으로 전자서명을 만들 수 있는 서명자와 서명 받을 메시지를 제공하는 송신자로 구성되어 있는 서명 방식으로, 송신자의 신원과 메시지, 서명 쌍을 연결시킬 수 없는 특성을 유지할 수 있는 서명이다. 은닉 서명은 서명하고자 하는 메시지의 내용을 공개하지 않고 메시지에 대한 서명을 받고자 할 때 사용된다. 서명자의 익명성과 송신자의 익명성을 보장함으로써 기밀성의 보장을 가능하게 하는 특수한 전자서명이다[7].

2.2.2 그룹 서명

그룹 서명은 1991년 David Chaum과 Eugene van

Heyst에 의해 처음 소개된 방법으로 그룹의 멤버들이 자신을 드러내지 않고 익명성을 유지하면서 서명을 제시하는 방법이다[4]. 그룹의 멤버만이 서명이 가능하며 서명을 받은 사람은 서명을 통해 서명자가 그룹의 멤버라는 사실은 알 수 있으나, 정확히 누구인지는 알 수 없다. 특별한 경우, 그룹 관리자는 서명을 개봉해서 누가 서명을 했는지 찾아내는 것이 가능하다. 그룹 서명은 그룹 관리자와 그룹 멤버로 구성되며, 기능적인 측면에서는 발행자, 개봉자, 검증자로 나누어 생각해 볼 수 있다. 그룹 서명의 프로토콜은 준비(Setup), 가입(Join), 서명(Sign), 검증(Verity), 개봉(Open)으로 총 5 단계의 과정을 포함하고 있다[8, 10]. 예를 들어 그림 1은 그룹 서명 과정을 나타낸다.



[그림 1] 그룹 서명 과정
[Fig. 1] Group signature process

2.2.3 링 서명

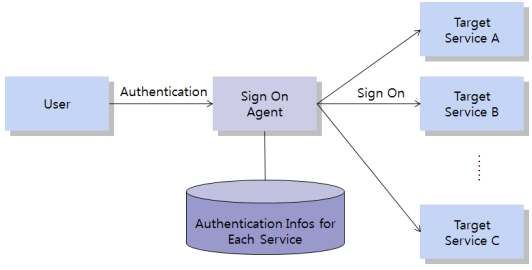
링 서명은 2001년 Ron Rivest, Adi Shamir, Yael Tuman에 의해 처음 소개된 방법으로 키를 가진 그룹 멤버들 중 어떤 사람에 의해서도 서명할 수 있고, 서명된 메시지는 특정 그룹 멤버들 중 한명에 의해 보증되는 방법이다[6]. 링 서명은 익명성을 폐기할 수 없고 그룹 관리자가 없다는 특징을 가지고 있다.

2.2.4 추적 가능한 서명

추적 가능한 서명은 2004년 Kiayiase 등이 제안한 방법으로 그룹 서명을 확장하여 익명성 관리에 대한 더욱 효율적인 공정성 메커니즘을 제공하는 방법이다[4]. 그룹 서명에서는 자신의 신원을 밝히기 위해서는 그룹 관리자가 서명을 열어보아야 하지만 추적 가능한 서명에서는 서명자가 원하는 경우 스스로 특정 서명에 대해서 자신이 서명한 것임을 밝힐 수 있도록 하였다.

2.3 SSO(Single Sign On)의 개념

SSO라는 단어의 의미는 한 번에 통합된 로그인을 말한다. 어떤 사용자가 로그온을 필요로 하는 복수개의 시스템을 동시에 사용하고자 할 경우, 이 사용자는 매 시스템마다 로그온을 해야 하는 불편함을 겪을 수 있다. 이때 어느 시스템이든 로그온이 되어 있으면 다른 시스템에서는 이 정보를 공유해서 별도의 로그온 과정을 거치지 않을 수 있다. 이렇게 되면 사용자는 중복 로그온의 과정을 거칠 필요가 없게 된다. 이러한 것을 시스템적으로 가능하게 해주는 것이 SSO이다[2, 5]. 간단히 여러 웹 서비스를 이용하는데 하나의 서비스에만 로그인을 하면 다른 서비스에는 로그인할 필요가 없이 바로 서비스를 이용 가능하다는 개념이다. 그림 2는 SSO를 보여주고 있다.



[그림 2] SSO(Single Sign On)
[Fig. 2] SSO(Single Sign On)

SSO 토큰은 쿠키를 통해 전달되므로 외부에 노출되는 정보이다. 완벽한 보안을 위해서는 토큰이 네트워크에서 노출되어서는 안 되지만, 비용 및 관리상의 이유로 허용되고 있다. 하지만 토큰을 통해 토큰이 포함하고 있는 정보까지 외부에 노출하는 것은 심각한 결함을 제공한다. 토큰의 네트워크 구간에서의 정보 노출 및 위·변조를 방지하기 위해 다음과 같은 보안 기술이 사용된다.

① Data Confidentiality

토큰은 주요 암호 알고리즘(AES, SEED)과 128bit 이상의 키로 암호화돼 보호되어야 한다.

② Data Integrity

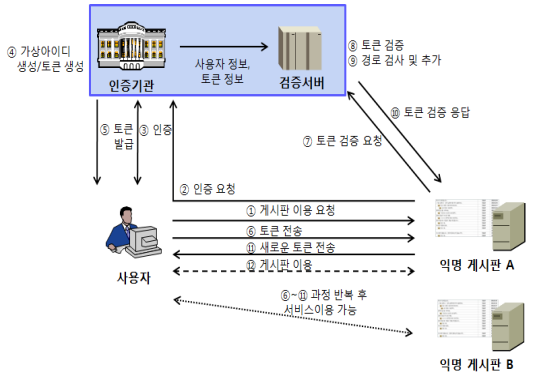
토큰은 MAC등을 포함해 데이터의 무결성을 보장해야 한다.

③ Replay Attack Protection

토큰은 사용자와 대상 어플리케이션 사이에 전달되는 인증 정보이다. 일반적으로 토큰은 네트워크에 노출되며, 노출된 토큰을 사용해 다른 사용자가 인증을 받고 들어올 수 있다. 이러한 문제점을 근본적으로 해결하기 위해서는 토큰을 네트워크에 노출시키지 않아야 한다. 토큰을

네트워크에 노출 시키지 않기 위해서는 항상 사용자와 대상 어플리케이션 사이에 암호 채널을 형성해야 하며, 이 채널을 통해 토큰을 전달해야 한다. 그러나 SSL과 같은 채널 암호를 사용하는 데에는 매우 많은 비용이 요구되어 실제로 많이 사용되지 있지는 않다. SSL과 같은 암호채널을 사용하지 않으면서 Replay Attack이 발생할 수 있는 상황을 줄일 수 있도록 Timestamp를 사용하여 임계시간을 넘으면 자동으로 토큰을 재발행하게 한다.

3. 제안하는 시스템



[그림 3] 시스템 구성도
[Fig. 3] System configuration

본 논문에서 제안하는 시스템의 전제 구성도를 그림 3에서 나타내었다. 사용자는 게시판 이용을 위해 익명 게시판 사이트에 접속하여 게시판 이용 요청을 한다. 이용요청을 받은 게시판 사이트는 사용자 인증을 위해 인증기관 사이트로 Redirection한다. 사용자는 아이디와 패스워드를 통해 인증기관에 사용자 인증을 받는다. 인증 후 인증기관은 가상 아이디 생성 방법을 통하여 가상 아이디를 생성하고 토큰을 생성하고 사용자에게 토큰을 발급한다. 토큰을 받은 사용자는 토큰을 익명 게시판으로 전송한다. 게시판 사이트는 토큰 검증을 위해 검증서버에게 토큰 검증 요청을 한다. 검증서버는 토큰 검증(전자서명 검증, 가상 아이디 검증) 과 경로 검증을 하고 토큰을 새로운 가상 아이디와 경로를 추가하여 갱신한다. 갱신된 토큰은 사용자에게 다시 전달되고 전달받은 토큰을 이용하여 단일 인증에 사용한다.

3.1 시스템의 구성요소

제안하는 시스템의 구성요소는 인증기관, 검증서버, 사용자, 익명게시판 사이트로 구성되어져 있고, 인증기관과 검증서버는 신뢰된 기관으로 크게는 인증기관, 사용자, 익명게시판 사이트 세부분으로 나눌 수 있다.

① 인증기관 및 검증서버

인증기관은 사용자 인증과 가상아이디와 경로를 가지는 토큰을 발급하는 기관이고 검증서버는 인증기관과 신뢰관계에 있는 서버로서 사용자 정보와 토큰정보를 가지고 토큰 검증 및 경로 추가를 한다.

② 사용자

익명게시판을 사용하고자 하는 사람으로서 XML로 전자 서명된 토큰을 가지고 게시판을 이용한다.

③ 익명게시판 사이트

익명 게시판 서비스를 제공하는 사이트로서 사이트는 사용자에 대한 어떠한 정보도 가지고 있지 않는다. 사이트는 단지 사용자로부터 받은 토큰을 검증서버에 검증요청을 하고 인증된 토큰에 대해서만 게시판 서비스를 제공하는 역할을 한다.

3.2 가상 ID발급과 경로 구성 기법

3.2.1 익명게시판 시스템의 토큰 구성

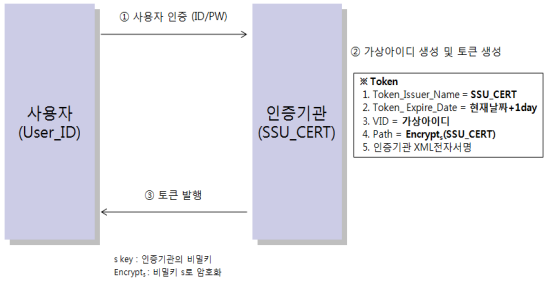
제안하는 토큰은 표 1과 같이 구성되어 있다. Token_Issuer_Name 필드는 토큰을 발급한 기관의 이름을 담고 있으며, 토큰을 발급한 기관은 최초 경로 아이디와 일치한다. Token_Expire_Date필드는 토큰의 만료기간을 담고 있으며 토큰의 만료기간은 발급한 시간부터 24시간이다. VID 필드는 가상 아이디가 들어가는 필드로서 실제로 토큰을 식별하는 역할을 수행하고 인증기관에 저장되어 있는 가상 아이디 비밀번호를 통하여 토큰검증에 사용되기도 한다. Path 필드는 경로가 들어가 있는 필드로서 경로는 기밀성을 위해 인증기관의 비밀키로 암호화되어 저장된다. 초기 값은 $Encrypt_s$(SSU_CERT)로서 s는 인증기관의 비밀키이고, SSU_CERT는 인증기관의 경로는 나타내는 유일한 아이디이다. 토큰의 모든 필드는 XML전자서명을 이용하여 기밀성과 무결성을 보장한다.

[표 1] 토큰 구성
[Table 1] Token configuration

필 드	설 명
Token_Issuer_Name	발급자 이름
Token_Expire_Date	토큰 만료 일자
VID	가상 아이디
Path	경로
인증기관 XML전자서명	

토큰 안에 가상 아이디 필드는 익명성을 제공하고 경로 필드는 조건부 추적을 가능하게 한다. 토큰을 가진 사용자는 토큰을 게시판 사이트로 보내고 토큰을 받은 사이트는 검증서버를 통해 토큰을 검증하고 새로운 가상아이디와 경로를 추가한 토큰을 발급받아 사용자에 제공하면 사용자는 타 사이트 이용 시 제공받은 토큰을 사용한다.

3.2.2 토큰 및 가상 아이디 생성



[그림 4] 가상 아이디 및 토큰 생성
[Fig. 4] Virtual IDs and Token generation

제안하는 시스템의 가상아이디는 그림 4와 같은 과정을 통해 생성된다.

과정 ① : 사용자는 아이디와 패스워드를 통해 인증기관에 사용자 인증을 받는다.

과정 ② : 인증기관은 토큰을 생성한다.

[표 2] 최초 토큰 구성
[Table 2] First token configuration

필 드	설 명
Token_Issuer_Name	SSU_CERT
Token_Expire_Date	현재날짜 + 1day
VID	가상 아이디
Path	$Encrypt_s$(SSU_CERT)
인증기관 XML전자서명	

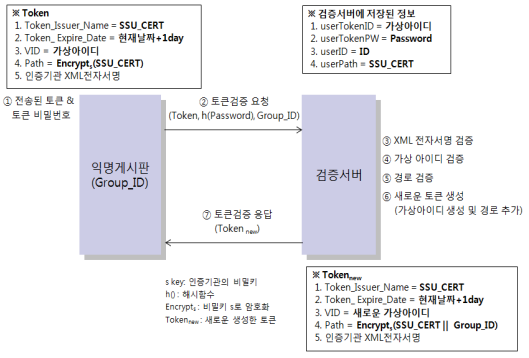
표 2는 인증기관에서 발행한 최초 토큰을 보여준다. Token_Issuer_Name은 토큰을 발급한 기관의 이름을 담고 있는 필드로서 SSU_CERT라는 인증기관 아이디를 담고 있고 Token_Expire_Date는 만료날짜를 담고 있는 필드로서 토큰을 발급하는 현재날짜 + 1day값은 담고 있다. VID는 가상 아이디를 담고 있는 필드로서 136개의 임의의 문자표에서 랜덤하게 16개의 문자를 뽑아 만든 가상 아이디를 담고 있다. 마지막으로 Path는 경로를 담고 있는 필드로서 최초 발급 시 경로는 인증기관부터 시작하므로 인증기관을 나타내는 아이디인 SSU_CERT를 담고 있다. 경로 필드는 나중에 경로 검증과 경로 추적 시 사용되는 중요한 정보임으로 토큰에 평문으로 저장할 수 없다. 때문에 경로필드는 인증기관만 알고 비밀키로 암호화 되어 저장된다. 경로를 암호화하기 위한 과정은 [식 1]과 같다.

$$Encrypt_s(SSU\_CERT) \quad (1)$$

여기서 s는 인증기관만 알고 있는 비밀키이고 SSU_CERT는 최초 경로인 인증기관의 아이디이다. Encrypt()는 암호화 알고리즘으로 256비트의 비밀키와 128비트의 IV(Initialization Vector)로 이루어진 대칭키 알고리즘인 AES를 제안하고 있다. 토큰의 모든 필드는 XML전자서명을 이용하여 서명되어 기밀성과 무결성을 보장한다.

과정 ③ : 생성한 토큰을 사용자에게 토큰을 발행한다.

3.2.3 토큰 검증 및 경로 구성



[그림 5] 토큰 검증 및 경로 구성 과정
[Fig. 5] Token verification and Path configuration

제안하는 시스템의 토큰 검증과 경로구성은 그림 5와 같은 과정을 통해 이루어진다.

[표 3] 전송된 토큰 구성
[Table 3] Transmitted token configuration

필 드	설 명
Token_Issuer_Name	SSU_CERT
Token_Expire_Date	현재날짜 + 1day
VID	가상 아이디
Path	$Encrypt_s$(SSU_CERT)
인증기관 XML전자서명	

과정 ① : 익명 게시판 사이트는 사용자로부터 인증기관에게 발급받은 토큰과 사용자가 알고 있는 비밀번호를 전송 받는다. 표 3은 사용자로부터 전송된 토큰을 보여준다.

과정 ② : 익명 게시판 사이트는 검증서버로 토큰 검증 요청을 하기위해 전송받은 토큰과 해시된 토큰 비밀번호, 사이트의 고유한 아이디인 Group_ID를 검증서버로 전송한다.

과정 ③ : 검증서버는 전송된 토큰을 검증하기 위해 첫 단계로 XML전자서명 검증을 한다. XML전자서명을 검증함으로써 토큰의 무결성을 보장할 수 있다.

과정 ④ : 무결성이 확인된 토큰에서 가상 아이디 검증을 위해 토큰의 VID필드에 있는 가상 아이디와 토큰과 같이 보내온 해시된 토큰 비밀번호를 가지고 아이디/패스워드 인증을 한다. 가상 아이디 검증은 인증기관에서 토큰을 발급하기 위해 쓰이는 아이디/패스워드가 노출되어 토큰이 발급 되었다 하더라도 토큰 비밀번호를 통해 다시 인증을 하기 때문에 Two Factor 인증효과를 얻을 수 있다.

과정 ⑤ : 가상 아이디 검증 후 마지막으로 경로 검증을 수행한다. 경로 검증은 토큰의 Path필드에 암호된 경로를 복호화하여 검증서버에 저장된 userPath와 비교한다. 경로 검증을 하기 위한 과정은 [식 2]와 같다.

$$Decrypt_s(Path) == userPath \quad (2)$$

경로 정보는 토큰이 사용되어진 사이트의 아이디 정보를 계속하여 업데이트하기 때문에 가로챈 토큰을 재사용하는 Replay Attack을 방지할 수 있다. 또한 법적인 문제시 경로 정보는 증거로 사용되어 질 수 있다.

과정 ⑥ : 새로운 토큰을 생성한다. 새로운 토큰을 생성하기 위해 앞 절에서 설명한 가상 아이디 생성 방법을 통해 새로운 가상 아이디를 생성하고 검증 요청 시 전송된 익명 게시판의 아이디인 Group_ID를 가지고 경로 추가를 한다. 경로 추가를 위한 과정은 [식 3]과 같다.

$$Encrypt_s(SSU\_CERT \parallel Group\_ID) \quad (3)$$

검증 서버에 저장된 경로 정보와 토큰에 경로는 동시 추가가 이루어 져야한다. 가상 아이디 생성과 경로 추가 후 새로 생성된 토큰 구성은 표 4와 같다.

[표 4] 새로 생성된 토큰 구성
[Table 4] Generated new token configuration

필 드	설 명
Token_Issuer_Name	SSU_CERT
Token_Expire_Date	현재날짜 + 1day
VID	새로운 가상 아이디
Path	$Encrypt_s$(SSU_CERT ‖ Group_ID)
인증기관 XML전자서명	

과정 ⑦ : 토큰 검증에 성공할 경우 새로 생성된 토큰을 전송한다.

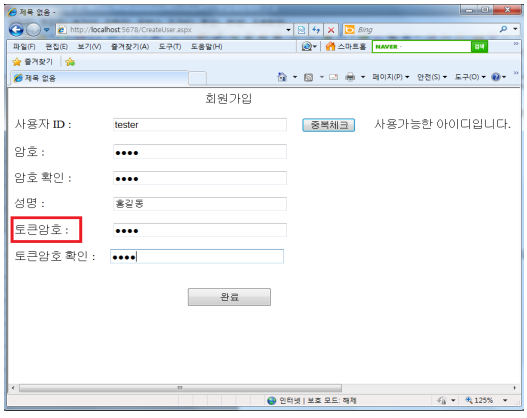
익명 게시판 사이트는 토큰검증 응답으로 받은 토큰을 사용자에게 돌려주고 사용자는 돌려받은 토큰을 사용하여 다른 게시판 사이트 이용 시 재사용하게 된다.

4. 구현 및 성능평가

본 장에서는 기존의 게시판 시스템과 제안하는 가상 ID 발급과 경로 구성 기법을 통한 익명 게시판을 비교 분석한다.

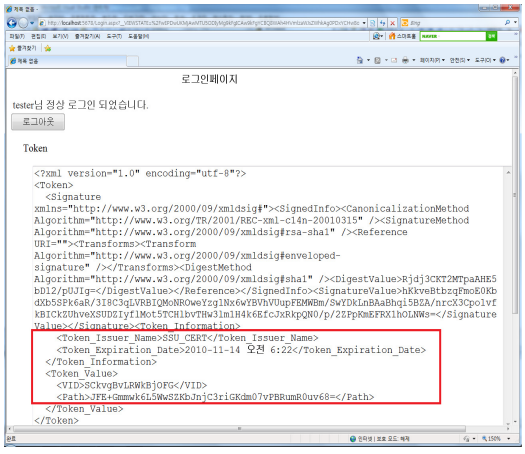
4.1 익명 게시판 서비스 구현

본 논문에서 구현된 시스템은 경로 암·복호화는 AES 256bit 대칭키 알고리즘을 사용하였고 XML 전자서명으로 RSA 1024bit 공개키 알고리즘을 사용하였다. 익명 게시판 서비스를 이용하기 위해서는 사용자는 게시판 사이트가 아닌 인증기관에 등록되어 있어야 한다.



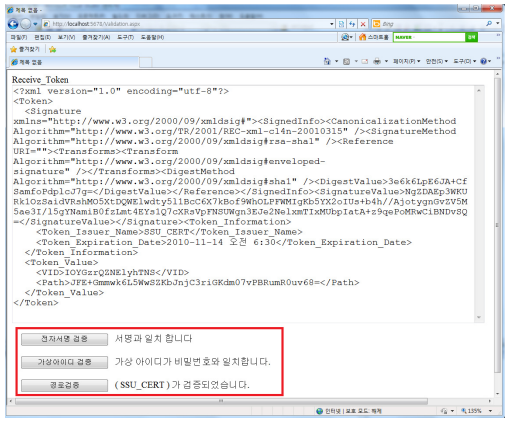
[그림 6] 인증기관 등록
[Fig. 6] Certificate authoritive registration

그림 6은 인증기관 등록을 나타내고 있다. 인증기관에 등록 정보는 간소화 하여 구현 하였다. 기존의 회원가입 페이지와 다른 점은 기존의 패스워드와 함께 토큰 암호도 입력을 받는다. 토큰 암호는 가상 아이디 검증에 사용하게 된다. 인증기관에 등록된 사용자는 아이디/패스워드 인증을 통해 로그인을 하면 토큰을 생성하게 된다. 토큰은 XML 데이터로 생성되고 XML 데이터는 XML 전자서명을 통해 무결성을 보장 받게 된다. 토큰은 3.2.1절의 토큰 구성과 같이 Token_Issuer_Name, Token_Expiration_Date, VID, Path로 구성되어 있다. Token_Issuer_Name는 인증기관의 아이디인 SSU_CERT를 담고 있고 Token_ Expiration_Date는 발급한 날짜의 다음날, VID는 136개의 임의의 문자표에서 랜덤하게 16개의 문자를 뽑아 만든 가상 아이디를 담고 있다. Path는 최초 경로인 SSU_CERT를 AES 알고리즘으로 암호화 하여 담고 있다. 그림 7에서 인증 후 토큰을 생성한 화면을 나타내었다.



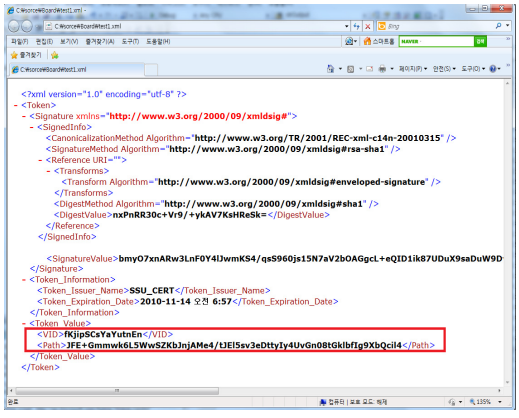
[그림 7] 토큰 생성
[Fig. 7] Token generation

토큰을 발급 받은 사용자는 익명 게시판에 발급 받은 토큰과 패스워드를 입력한다. 토큰과 토큰 패스워드를 받은 익명 게시판 사이트는 토큰 검증을 검증 서버로 요청하게 되고 검증 서버에서 토큰 검증을 마치고 나면 게시판 서비스를 이용하게 된다. 검증 과정은 익명 게시판 사이트와 검증 서버 사이에서 이루어진다. 검증 과정은 XML 전자서명 검증, 가상 아이디와 비밀번호 인증, 경로 검증 총 3단계로 이루어진다. XML 전자서명 검증을 통해 토큰의 무결성을 제공하고, 가상 아이디 검증을 통해 아이디/패스워드가 노출되어 토큰이 발급 되었다 하더라도 토큰 비밀번호를 통해 다시 인증을 하는 Two Factor 인증효과를 얻을 수 있으며, 경로 검증은 Replay Attack을 방지하고 법적인 문제시 증거가 될 수 있다. 그림 8은 토큰 검증 페이지이다.



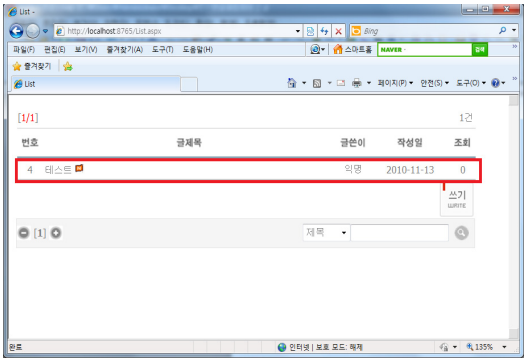
[그림 8] 토큰 검증
[Fig. 8] Token verification

검증이 완료되면 검증 서버는 새로운 가상 아이디와 경로를 추가한 토큰을 익명 게시판에게 전송한다. 사용자는 익명 게시판으로부터 새로 갱신된 토큰과 함께 서비스를 제공 받고 갱신 토큰을 재사용하여 단일 인증 기능을 제공하게 된다.



[그림 9] 사용자 토큰
[Fig. 9] User's token

그림 9는 사용자가 새롭게 발급받아 저장하고 있는 XML 토큰을 나타내고 그림 10은 제안하는 익명 게시판 시스템을 이용하여 익명 인증 후 게시판에 글을 등록한 화면이다.



[그림 10] 게시판 서비스
[Fig. 10] Bulletin board service

4.2 기존 시스템과의 비교 분석

현재 게시판 서비스는 개인정보 등록 및 확인 과정을 통해 사용자 인증을 하고 있다. 이러한 실명 인증은 불필요하게 과도한 사용자의 개인정보를 요구하여 개인 사생활을 침해하고, 부주의한 정보관리로 인해 대량의 개인정보 유출의 근원이 되었다. 이와 같은 문제점을 해결하기 위해 실명제와 완전한 익명성이라는 양극단적인 접근법의 보완재적 역할을 수행할 수 있는 익명 인증 기술에 관한 연구가 활발하게 이루어지고 있다. 표 5는 기존 게시판 기술과 제안하는 게시판 기술의 특징을 비교하였다.

[표 5] 특징 비교
[Table 5] Feature comparison

비교항목	그룹 서명을 이용한 익명게시판	제안하는 익명게시판
익명성	지원	지원
책임 추적성	지원	지원
인증기관	필요	필요
개인정보관리	통합관리	통합관리
보안기법	그룹 서명방식	보안토큰방식
단일인증	미지원	지원

제안하는 익명게시판과 기존의 게시판 시스템의 특징을 비교하면 기존의 실명 게시판은 익명성을 제공하지 않기 때문에 인증기관이 불필요하나 그룹 서명을 이용한 익명 게시판과 제안하는 익명 게시판의 경우는 익명성을 제공하면 책임 추적성도 제공하기 위해 인증기관이 필요하다. 실명 게시판의 경우 개인정보 등록 및 확인 과정을 통해 책임 추적성을 제공하기 때문에 각 웹 사이트마다 개인 정보가 중복적으로 존재한다. 개인 정보의 분산은 개인 정보 관리의 어려움과 유출 가능성을 높인다. 하지만 그룹 서명을 이용한 익명 게시판과 제안하는 익명 게시판의 경우는 개인 정보를 인증기관에서 통합적으로 관리하고 불필요한 개인 정보노출을 피하면서 사용자의 정당성을 각 게시판 사이트로 제공한다.

그룹 서명을 이용한 익명 게시판과 제안하는 익명 게시판의 차이점은 보안기법에서 그룹 서명을 이용한 익명 게시판은 그룹 서명 방식을 제안하는 익명 게시판은 XML 보안 토큰 방식을 사용한다는 점이다. 때문에 그룹 서명을 이용한 익명 게시판의 경우는 사용자가 그룹 인증기관에게 그룹 멤버키를 발급 받아 그룹 서명 후 게시판 사이트에 전송하기 때문에 타 게시판을 이용 시 사용자가 매번 서명을 해야 하는 단점이 있다. 하지만 제안하는 익명 게시판의 경우 XML 보안 토큰 방식을 사용한다. XML 보안 토큰의 무결성을 위해 XML 전자서명을 사용하지만 서명을 사용자가 하는 것이 아니라 인증기관에서 서명 후 발급하기 때문에 사용자의 부담 적다. 또한 보안 토큰을 사용하기 때문에 단일 인증이 가능하여 타 게시판 이용 시 재사용 할 수 있다는 장점이 있다.

4.3 제안하는 시스템의 성능 평가

제안하는 시스템의 성능 평가는 실명 추적이 가능한 익명 게시판이라는 전제하에 이루어진다. 때문에 비교 대상은 그룹 서명을 이용한 익명게시판과 비교하였다.

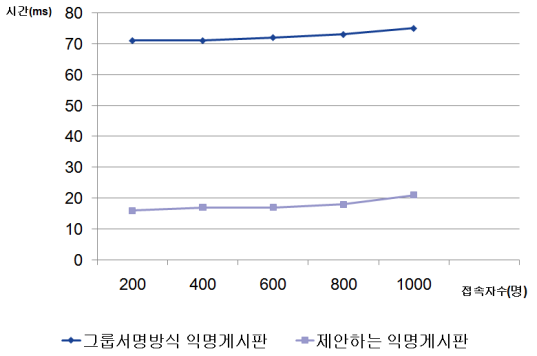
표 6은 프로토콜 성능에 가장 큰 영향을 주는 암호화 기법에 따른 성능을 비교한 것이다. 그룹 서명을 이용한 익명 게시판은 그룹 서명을 적용하기 때문에 그룹 서명 기법의 계산 효율성이 프로토콜의 성능에 큰 영향을 준다. 그룹 서명 등에 사용되는 bilinear pairing 연산은 기존의 지수승, 대칭키 암호화 보타 무거운 연산으로 알려져 있다. 특히 pairing 기반의 Boneh 등의 기법은 자주 쓰이는 값을 선 계산하는 방법으로 필요한 연산회수를 최적화 하면 서명 계산 시 8번의 지수승 연산이 소요되고 서명 검증 시 6번의 지수승연산과 1번의 pairing 연산이 필요하다.

[표 6] 성능 비교
[Table 6] Performance comparison

비교항목	그룹 서명을 이용한 익명게시판	제안하는 익명게시판
암호화 기법	Group Signature	RSA Signature
키 길이	1533 bit	1024 bit
서명 계산 시 지수승 연산	8회	1회
서명 검증 시 지수승 연산	6회	1회
Pairing 연산	1회	안함
서명 시간	약 0.32 sec	약 0.06 sec
서명 검증 시간	약 0.36 sec	약 0.03 sec

제안하는 익명게시판의 경우는 그룹 서명 방식이 XML 전자서명을 이용한 보안 토큰 방식을 사용한다. XML 전자서명의 암호화 방식은 일반적으로 RSA Signature를 사용한다. RSA Signature는 서명 계산 시 1번의 지수승 연산이 소요되고 서명 검증 시 1번의 지수승 연산이 소요된다. RSA Signature에서 서명시간과 검증시간이 차이가 나는 이유는 일반적으로 공개키는 개인키보다 작은 비트를 사용하기 때문이다.

이와 같이 제안하는 익명게시판은 그룹 서명 방식이 아닌 XML 전자서명을 이용한 보안 토큰 방식을 사용하기 때문에 효율성 면에서 기존의 방식보다 뛰어나다.



[그림 11] 인증시간 평가
[Fig. 11] Verification time evaluation

그림 11에서 접속자 수에 따른 인증시간의 성능 평가 결과를 제시하였다. 즉, 게시판 서버에 접속하는 동시 접속자 수를 200명, 400명, 600명, 800명, 1000명으로 나누고 인증방식에 따라 측정한 동시 접속자 중 1인의 인증시간을 그래프로 나타냈다. 성능분석 결과 접속자 수에 따른 인증시간에서 그룹 서명 방식을 사용한 익명 게시판은 평균 응답 속도가 0.72초, 제안하는 방식은 0.18초를 나타내었으며, 결과적으로 인증시간에서 4~5배 정도 빠른 응답 속도를 보임을 알 수가 있다. 접속자 수에 따른 인증시간은 미세하게 증가하나 대체로 일정하다고 볼 수 있다. 이와 같은 빠른 응답 속도는 빈번한 사용이 이루어지는 익명 게시판 서비스에서 그룹 서명을 이용한 익명 게시판 시스템보다 제안하는 시스템이 게시판에 적용하기에 더 적합함을 보여준다.

5. 결 론

본 논문에서는 SSO의 기술 중 하나인 XML 토큰 방식을 사용하여 개인정보의 분산을 막고 단일 로그인이 가능하게 하였고 토큰 발급 시 가상 아이디와 경로구성을 통해 익명성 및 조건부 추적이 가능한 익명 게시판을 제안 하였다. 기존 인증 방식의 문제점을 개선하여 제안하는 방식을 사용하는 경우 단일 인증을 제공하면서도 키 길이가 1533bit에서 1024bit로 짧아졌으며 연산과정 역시 간단해진다.

성능분석 결과 접속자 수에 따른 인증시간에서 그룹 서명 방식을 사용한 익명 게시판은 평균 응답 속도가 0.72초, 제안하는 방식은 0.18초를 나타내었다. 즉 인증시간에서 4~5배 정도 빠른 응답 속도를 보였다. 또한 제안하는 시스템은 단일 인증을 제공하고 사용자가 서명을 하지 않아도 되기 때문에 사용자 편의성에서 월등히 뛰어났다. 이와 같은 사용자 편의성은 익명 게시판에 제안하는 시스템이 더 적합함을 보여준다.

보안성 측면에서는 기존의 인증방식은 사용자가 그룹 서명하는 방식을 사용하기 때문에 보안강도에서 월등하다. 제안하는 시스템에서는 보안 강도를 높이기 위해 3단계의 검증한다. 인증기관의 서명 검증을 통해 토큰의 무결성을 제공하고, 가상 아이디 검증을 통해 Two Factor 인증효과를 얻을 수 있으며, 경로 검증은 Replay Attack을 방지하고 법적인 문제시 증거가 될 수 있다. 이와 같은 3단계의 검증을 통해 보안 강도가 향상 되었다.

익명 게시판의 문제점인 악성 댓글 폭력과 존재하지 않는 허위 사실 유포 등의 인터넷 역기능을 막기 위해 제안하는 시스템을 사용할 경우 검증 서버를 통해 기존 문제점을 막을 수 있으며 빠른 응답 속도와 간단한 연산과정은 익명성을 유지하면서도 사용자의 불편함을 못 느끼게 할 것이다.

제안하는 시스템은 게시판 서비스에 국한되지 않고 전자투표, 전자입찰 등 익명성이 요구되는 다양한 분야에서 사용할 수 있는 효과를 기대할 수 있다. 그러므로 향후에는 보안 강도를 향상시키기 위한 연구를 수행할 계획이다.

References

[1] Tae-Kyoung Kwon. et al., “The Technology and Trend of Public Key based Bulletin board”, Journal of KIISC, Vol.14, No.6, pp.1-13, 2004.

[2] Jae-Hyung Yoo, “Recent Development of Integrated Identity Management Technologies to realize Multi-Domain Single Sign On”, KNOM Review, Vol.10, pp.16-31, 2007.

[3] Dong-Young Cho, “Design of a Web-bulletin board System Using Anonymous Authentication of a Group Membership”, Journal of KI-IT, Vol.8, No.2, pp.95-100, 2010.

[4] Seung-Geol Choi. et al., “Anonymity Mechanisms : Group Signatures and Traceable Signatures”, Journal of KIISE, Vol.24, No.1, pp.32-39. 2005.

[5] Jin-Tak Choi, “A Study on Authentication Management Technique Used of SSO”, KSIAM IT series, Vol.10, No.1, pp.61-69, 2006.

[6] Yun-Kyung Lee. et al., “The Technology and Trend of Anonymous Authentication”, ETRI, Vol.23, No.4, pp.19-29, 2008.

[7] D. Chaum, “Blind signature systems”, In Advances in Cryptology-CRYPTO'83, p.153. Plenum, 1983.

[8] D. Chaum and E. van Heyst. “Group signatures", EUROCRYPT 1991, LNCS, Springer., 1991.

[9] Jan Camenisch and Anna Lysyanskayas, “An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation”, EUROCRYPT 2001, LNCS 2045, 2001.

[10] M. Bellare, D. Micciancio, and B. Warinschi, “Foundations of Group Signatures: Definition, Simplified Requirements and a Construction Based on General Assumptions”, CRYPTO 2004, 2004.

[11] Rabin, Michael. “Digitalized Signatures and Public-Key Functions as Intractable as Factorization”. MIT Laboratory for Computer Science, 1979.

[12] Jun young Heo, “QoS-guaranteed Routing for Wireless Sensor Networks”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL. 11, No. 6, December, 2011.

[13] Sun-Jin Oh, “Design and Evaluation of a Weighted Intrusion Detection Method for VANETs”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.11, No.3, June, 2011.

[14] Sun-Jin Oh, “An Anomaly Detection Method for the Security of VANETs”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.10, No.2, April, 2010.

[15] Young-Hee Cho, Gye-Sung Lee, “Prediction on Clusters by using Information Criterion and Multiple Seeds”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.10, No.6, December, 2010.

[16] Ho-Young Hwang, Hyo-Joong Suh, “The Multi-path Power-aware Source Routing(MPSR) for the Maximum Network Lifetime in Ad-Hoc Networks”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.10, No.5, October, 2010.

[17] Eun Cheol Kim, Seo Sung Il and Jin Young Kim, “Performance of Tactics Mobile Communication System Based on UWB with Double Binary Turbo Code in Multi-User Interference Environments”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.10, No.1, February, 2010.

[18] Ju phil Cho, Sang-In Cho, Kyu-Min Kang, Heon-Jin Hong, “Analysis on Characteristics for Sharing Co-channel between Communication Systems”, Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.11, No.4, August, 2011.

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

장 승 재(Seung-Jae Jang) **[정회원]**

- 2009년 2월 : 숭실대학교 컴퓨터학부 (공학사)
- 2011년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2011년 3월 ~ 현재 : 숭실대학교 컴퓨터학과(박사과정)

<관심분야>
정보통신, 정보보안